GUIA DE SEGURANÇA DE UM HACKER // INFOGRÁFICO 01/08

PHISHING E GOLPES: ANATOMIA DE UMA FRAUDE

Os atacantes imitam seu banco, suas redes sociais ou seu provedor para roubar seus dados e seu dinheiro. Aprenda a reconhecer o golpe antes de clicar.

>> SINAIS DE ALERTA

01 Urgência artificial
"Aja agora ou sua conta será bloqueada". Querem que você aja sem pensar.

02 Prêmios e dinheiro fácil
"Você ganhou um prêmio, informe seus dados para resgatá-lo". Exploram a ambição.

03 Endereço quase idêntico
www.faceb00k.com em vez de facebook.com: zeros que parecem letras "o".

04 Links encurtados
bit.ly/Ub1XC1 esconde o destino real. O navegador pode acabar em outro site.

05 Anexos inesperados
Arquivos que, ao serem abertos, instalam malware e roubam seus dados.

06 Visual "oficial"
Usam logos, textos e estética reais da empresa. Parecer bem-feito não prova nada.

>> VARIANTES DO MESMO Ggolpe

PHISHING – e-mail

SMISHING – SMS / WhatsApp

QUISHING – códigos QR falsos em parquímetros, restaurantes e mensagens

>> PROTOCOLO DIANTE DE QUALQUER MENSAGEM SUSPEITA

1. **Sempre desconfie**
Desconfie de toda mensagem que receber, de conhecidos ou não. Pense duas vezes antes de clicar.

2. **Não clique nem abra anexos de desconhecidos**
O ideal é ignorá-los diretamente.

3. **Nunca entregue seus dados por mensagem**
Os serviços legítimos não pedem usuário e senha dessa forma.

4. **Verifique pelo canal oficial**
Na dúvida, ligue para a empresa para confirmar se a mensagem é verdadeira.

5. **Inspecione o endereço exato**
Antes de digitar seus dados, confirme que a URL coincide exatamente com a do site verdadeiro.

REGRA DE OURO

Sempre desconfie e depois verifique antes de confiar.

A ESCADA DE PROTEÇÃO: DA SENHA ÀS PASSKEYS

Cada nível que você sobe reduz drasticamente a chance de roubarem uma conta sua. Identifique em qual degrau você está hoje.

>> SUBA DE NÍVEL

NÍVEL 0 — ZONA DE RISCO

Senha fraca ou reutilizada

Formada por dados pessoais, fácil de adivinhar, ou a mesma em vários serviços: se uma for comprometida, caem todas.

NÍVEL 1

Senha forte

Maiúsculas, minúsculas, números e caracteres especiais. Use uma regra mnemônica: por exemplo, as primeiras letras de uma frase.

NÍVEL 2

Única por serviço + gerenciador de senhas

Uma senha diferente em cada sistema. Com muitas contas, um gerenciador de senhas lembra delas por você.

NÍVEL 3

Autenticação multifator (MFA)

Um segundo fator além da senha: mesmo que a roubem, não basta para entrar.

NÍVEL 4 — OBJETIVO

Passkeys

Acesso sem senha, vinculado ao seu dispositivo: não há nada para roubar nem para adivinhar por phishing.

>> REGRAS QUE VALEM EM TODOS OS NÍVEIS

→ Não compartilhe suas senhas

Se por urgência você precisou compartilhar uma, troque-a imediatamente depois.

→ Perguntas de segurança difíceis

Se qualquer um pode respondê-las com dados públicos sobre você, elas são uma porta de entrada.

→ Não anote senhas em papéis nem arquivos

Nem cadernos, nem notas do celular. Se não houver outro jeito, guarde o papel em um lugar muito seguro.

→ Troca urgente diante de atividade estranha

Se notar movimentações estranhas em uma conta, troque a senha imediatamente. E renove suas senhas de tempos em tempos, sem esperar o sistema obrigar.

ATENÇÃO

Cuide para que ninguém observe você digitando sua senha: os olhares também roubam senhas.

GUIA DE SEGURANÇA DE UM HACKER // INFOGRÁFICO 03/08

SEU CELULAR É SUA VIDA: 10 PROTEÇÕES ESSENCIAIS

Fotos, contas, banco, mensagens: tudo vive no seu telefone. Estas dez medidas cobrem roubo, perda, apps maliciosos e golpes.

01 Bloqueio com código + bloqueio automático

Que só possa ser usado com seu código ou senha, e se bloqueie sozinho quando você parar de usá-lo.

02 Criptografia de dados

Habilite a criptografia dos dados internos e dos cartões de memória.

03 PIN no chip (SIM)

Sem PIN, sua linha pode ser usada em outro aparelho para receber seus códigos de verificação.

04 Rastreamento e apagamento remoto

Software que permita localizar o aparelho e, se for preciso, bloqueá-lo e apagar os dados a distância.

05 Apps só de lojas oficiais

Passaram pela verificação da empresa e da comunidade. Fora delas, território de malware.

06 Avaliações, downloads e permissões

Confira as avaliações e o número de downloads antes de instalar. Se as permissões forem excessivas, não continue: consulte alguém com experiência.

07 Atualizações em dia

Sistema operacional e aplicativos atualizados fecham vulnerabilidades conhecidas.

08 Carregamento seguro

Não carregue em qualquer lugar. Em USBs públicos, use proteção e o modo somente carga, sem sincronizar dados.

09 Tela discreta

Filtro de privacidade contra olhares curiosos e notificações limitadas com o aparelho bloqueado.

10 Backups + limpeza

Backup regular. Transfira o conteúdo sensível para o computador e apague-o do telefone.

>> BÔNUS: GOLPES POR MENSAGEM DE TEXTO

Smishing

Os mesmos golpes do phishing chegam por SMS e mensageiros: prêmios, "problemas com sua conta", encomendas. Aplique o mesmo protocolo: desconfiar, não clicar, verificar pelo canal oficial.

SE VOCÊ PERDER OU ROUBAREM SEU CELULAR

Com os itens 1–4 ativados, suas informações ficam protegidas mesmo sem o aparelho em seu poder.

LAR DIGITAL SEGURO: WI-FI, IOT E COMPUTADORES

As ameaças também chegam à sua casa de forma remota, pela internet e pelas redes sem fio. Quatro zonas a proteger.

ZONA 1 O roteador Wi-Fi

É a porta de entrada da sua casa digital. Configure-o de forma segura escolhendo as opções adequadas; se não souber como, consulte um técnico. Uma rede sem proteção permite que um intruso acesse seus dispositivos e dados.

ZONA 2 Dispositivos IoT

Câmeras, caixas de som, tomadas e eletrodomésticos inteligentes podem ser um canal de acesso à sua rede. Escolha-os e instale-os com cuidado, troque as senhas padrão e mantenha-os atualizados.

ZONA 3 Os computadores

Manutenção preventiva: evite infecções por malware e mau funcionamento. Antivírus ativo, sistema atualizado, downloads só de fontes seguras.

ZONA 4 Suas informações

Backups regulares: defina quais arquivos proteger, onde e com que frequência. A nuvem sozinha não basta.

>> O PLANO DE BACKUP EM 3 PERGUNTAS

Q?

O quê?

As informações que você não pode se dar ao luxo de perder: documentos, fotos da família, arquivos de trabalho.

O?

Onde?

Sempre em mais de um lugar, esteja ou não na nuvem. Se a nuvem falhar ou você perder o acesso, a cópia local salva você.

F?

Com que frequência?

Com uma frequência definida e regular, conforme o quanto suas informações mudam. Não "quando eu lembrar".

REGRA DOS DOIS LUGARES

O que é importante vive sempre em pelo menos dois lugares. **Todo o resto é opcional; isto não.**

GUIA DE SEGURANÇA DE UM HACKER // INFOGRÁFICO 05/08

ROUBO DE IDENTIDADE E PROTEÇÃO DO DINHEIRO

É um dos crimes que mais crescem no mundo: roubam seus dados pessoais para cometer fraudes em seu nome. Recuperar-se é muito difícil; prevenir é a jogada certa.

>> O QUE OS ATACANTES BUSCAM

- DOCUMENTOS DE IDENTIDADE (RG, CPF)
- CARTÕES DE CRÉDITO E DÉBITO
- RECIBOS E CONTAS DE SERVIÇOS
- SEUS DADOS DIGITAIS

>> LINHA DE DEFESA: PREVENIR → DETECTAR → REAGIR

1 **PREVENIR — Cautela com suas informações privadas**

Evite que seus dados e documentos pessoais caiam em mãos de terceiros. Não publique dados de identificação, destrua papéis com informações sensíveis antes de jogá-los fora e apresente seus documentos só quando for imprescindível.

▼

2 **DETECTAR — Monitore contas e cartões**

Confira movimentações e faturas com regularidade. Cobranças desconhecidas, por menores que sejam, são o primeiro sinal: os atacantes testam com valores pequenos, de R$ 5 ou R$ 10, antes do golpe grande. Ative alertas de gastos se o seu banco oferecer.

▼

3 **REAGIR — Rápido e com ajuda profissional**

Se descobrir que é vítima: consulte com urgência um especialista e tome medidas imediatas para evitar que o problema cresça. Avise o banco, bloqueie os cartões, troque as senhas das contas vinculadas.

>> PROTEJA O DINHEIRO NO DIA A DIA

→ Compras online só em sites confiáveis

Verifique o endereço exato da loja antes de digitar os dados do cartão.

→ Nunca dê dados bancários por mensagem ou telefone

Seu banco não pede senhas, tokens nem códigos por esses canais.

→ Não perca seus cartões de vista

Em lojas e restaurantes, que o cartão não desapareça do seu campo de visão.

→ Cuide dos papéis tanto quanto do digital

Recibos, contas e faturas contêm dados que servem para se passar por você.

POR QUE ISSO IMPORTA

De um roubo de identidade é muito complicado se recuperar: podem endividar você e cometer crimes em seu nome.

MENORES SEGUROS NA INTERNET: GUIA PARA PAIS E EDUCADORES

A meta não é proibir a tecnologia, e sim acompanhar: os menores podem saber mais de tecnologia que um adulto, mas não dos seus riscos.

>> OS 3 RISCOS QUE VOCÊ PRECISA CONHECER

CYBERBULLYING

Assédio entre pares por meios digitais. Peça que **informem qualquer assédio** ou pedido que pareça estranho ou desagradável.

GROOMING

Adultos que se passam por menores para ganhar a confiança deles. Verifique seus contatos; que **não falem com estranhos** nem usem seus nomes reais em chats de jogos.

SEXTING

Circulação de material íntimo. A regra tem três partes: **não produzir, não compartilhar e não pedir**.

>> O QUE FAZER / O QUE EVITAR

[+] FAZER

- » **Controle parental** e limites de uso, em especial com crianças pequenas
- » **Dispositivos em áreas comuns** da casa, não nos quartos
- » **Diálogo aberto** em família e na escola sobre o que veem e vivem online
- » **Ensinar os riscos** como parte da educação deles
- » **Dar o exemplo**: suas ações nas redes devem ser coerentes com o que você transmite a eles

[−] EVITAR

- × **Negar o acesso à internet**: ela é fundamental para o aprendizado e o futuro deles
- × **Deixar que compartilhem dados de identificação**: endereço, telefone, escola
- × **Operações com dinheiro** online antes de terem idade e critério para fazê-las sem risco
- × **Supor que "sabem mais que você"**: dominam a ferramenta, não o perigo
- × **Vigiar sem conversar**: o controle sem diálogo os empurra para o segredo

>> POR FAIXA ETÁRIA

−10 — **Crianças pequenas**
Controle parental ativo, acompanhamento direto, conteúdos filtrados, tempo limitado.

10+ — **Adolescentes**
Autonomia guiada: menos filtro, mais conversa. Que saibam que podem contar qualquer coisa a você **sem castigo por falar**.

PARA TRANSMITIR A ELES

Cuide do seu presente: no futuro ele será seu passado e, se estiver na internet, qualquer um poderá revisá-lo.

GUIA DE SEGURANÇA DE UM HACKER // INFOGRÁFICO 07/08

VOCÊ FOI HACKEADO? PROTOCOLO DE RESPOSTA

Roubo de conta, fraude, falsificação de identidade: o que você faz nas primeiras horas define o tamanho do dano. Siga esta ordem.

1 **NÃO apague nada — preserve as evidências**

Não apague nem reencaminhe e-mails, mensagens ou informações do incidente. Guarde tudo o que possa servir como prova: capturas de tela, e-mails, conversas.

▼

2 **Registre a ocorrência o quanto antes**

Na delegacia mais próxima da sua casa, ou na delegacia especializada em crimes cibernéticos. O boletim de ocorrência habilita a investigação e protege você se cometerem crimes em seu nome.

▼

3 **Corte o acesso do atacante**

Troque com urgência as senhas comprometidas e as das contas vinculadas (principalmente o e-mail principal: a partir dele se redefine todo o resto). Encerre as sessões abertas em todos os dispositivos.

▼

4 **Contate o provedor pelos canais oficiais**

Formulário, suporte ou telefone do serviço. Vão pedir dados para verificar que você é o dono: data estimada de criação, contatos frequentes, conteúdo dos últimos e-mails, pastas e marcadores. Em serviços gratuitos a resposta pode demorar: insista.

>> O QUE NÃO FAZER

[−] ERROS QUE PIORAM TUDO

- × Contratar um "hacker" para recuperar a conta: é ilegal se não for pelos meios do provedor, e costuma ser outro golpe
- × Reencaminhar ou divulgar o conteúdo do incidente
- × Esperar que a lei resolva sozinha: o papel ativo na proteção é seu

>> PREVENIR HOJE PARA RECUPERAR AMANHÃ

ATIVE A MFA | CADASTRE DADOS DE RECUPERAÇÃO | SEGUNDO ADMINISTRADOR DO PERFIL | BACKUP DO PERFIL (BAIXE SEUS DADOS)

REGRA

Evidências primeiro, ocorrência rápido, senhas novas já. Nessa ordem e sem demora.

GUIA DE SEGURANÇA DE UM HACKER // INFOGRÁFICO 08/08

FORA DE CASA: WI-FI PÚBLICO, CONEXÕES E VIAGENS

Cafés, aeroportos e hotéis são território compartilhado: redes que você não controla e aparelhos expostos. Condutas corretas para cada cenário.

>> TRÊS CENÁRIOS, UMA REGRA

CAFÉ / SHOPPING

- × Nada de **banco ou compras** em Wi-Fi alheio se você não confia na rede ou no provedor
- » Na dúvida, use **seus dados móveis**
- » Não deixe o aparelho sozinho **nem por um minuto**

AEROPORTO

- × **USBs públicos de carga**: podem sincronizar dados
- » **Carregador próprio** na tomada, ou **modo somente carga** com proteção
- » Verifique o **nome exato** da rede oficial antes de se conectar

HOTEL

- × Não deixe dispositivos **à vista** no quarto
- » **Cofre** para o que você não leva com você
- » **Sessões encerradas e aparelho bloqueado** sempre

>> ANTES DE VIAJAR: CHECKLIST DO APARELHO

1. **Backup completo**
   Se o aparelho for perdido ou roubado, suas informações continuam existindo.

2. **Criptografia de disco ativada**
   Medida de segurança avançada: sem a sua chave, o conteúdo do aparelho **é ilegível**.

3. **Localização de aparelhos ligada**
   Rastreamento, bloqueio e apagamento remoto disponíveis a partir de outro dispositivo.

4. **Viaje leve de dados**
   Leve no dispositivo **só o necessário**: o que não está nele não pode ser roubado.

>> EM TODO LUGAR PÚBLICO

→ Olhares curiosos

Filtro de privacidade na tela e cuidado ao digitar senhas cercado de gente: **não seja óbvio ao digitá-las**.

→ Proteção física

O roubo do aparelho continua sendo o ataque mais comum. **Junto ao corpo ou trancado**, sem exceções.

REGRA DO TERRITÓRIO COMPARTILHADO

Em redes que você não controla, comporte-se como se alguém estivesse observando. Às vezes é verdade.